(3)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-189823
(43)Date of publication of application : 05.07.2002

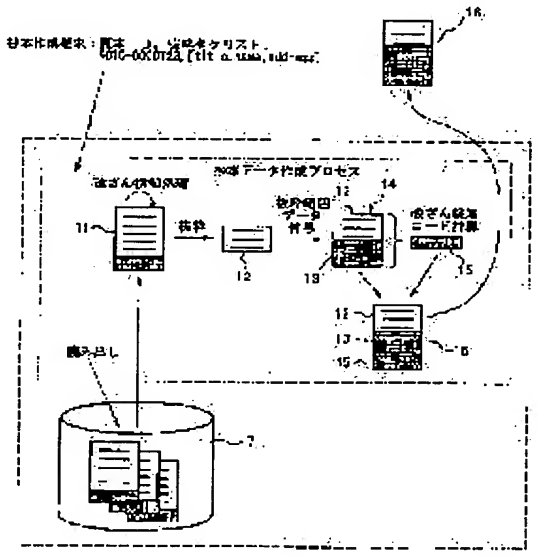
(51)Int.Cl. G06F 17/60
G06F 12/00
G06F 12/14
G09C 1/00
// G06F 17/30

(21)Application number : 2000-389177
(22)Date of filing : 21.12.2000

(71)Applicant : RICOH CO LTD
(72)Inventor : KANAI YOICHI
YANAIDA MASUYOSHI

(54) ABSTRACT DATA GENERATING METHOD, ABSTRACT DATA GENERATING DEVICE, DEVICE FOR IT, PROGRAM, AND STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an abstract data generating method generating credible abstract data from original data.
SOLUTION: When an abstract generation request including an original ID and an extraction tag list is received, the original data 11 specified by the original ID are read from an original storage medium 7, and an original data falsification detecting process is applied to the original data 11. If no falsification is detected, the data corresponding to the tag specified by the extraction tag list are extracted from the read original data as extracted data 12. The original ID and the extraction tag list are combined to form extraction range data 13, and the extracted data 12 and the extraction range data 13 are combined to form abstract contents data 14. An abstract falsification detection code calculation process is applied to the abstract contents data 14 to obtain a falsification detection code 15, and the abstract contents data 14 and the falsification detection code 15 are combined to form abstract data 16. The abstract data 16 are finally returned to an abstract generation requester.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－189823
（P2002－189823A）
(43)公開日　平成14年７月５日(2002.7.5)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
Ｇ０６Ｆ	17/60	１４０	Ｇ０６Ｆ 17/60	１４０	５Ｂ０１７
		１５４		１５４	５Ｂ０７５
		５１２		５１２	５Ｂ０８２
	12/00	５３７	12/00	５３７Ｈ	５Ｊ１０４
	12/14	３１０	12/14	３１０Ｚ	

審査請求　未請求　請求項の数12　ＯＬ　（全 10 頁）　最終頁に続く

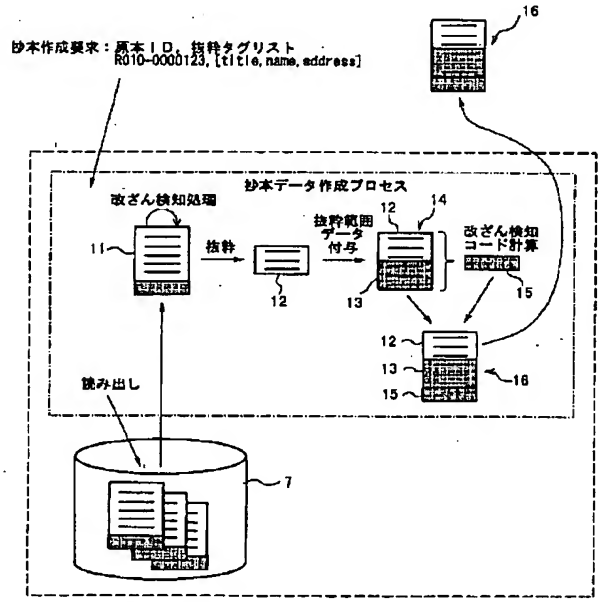
(21)出願番号　特願2000－389177(P2000－389177)
(22)出願日　平成12年12月21日(2000.12.21)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(72)発明者　金井　洋一
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(72)発明者　谷内田　益義
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(74)代理人　100079843
弁理士　高野　明近　（外２名）

最終頁に続く

(54)【発明の名称】　抄本データ作成方法、抄本データ作成装置、そのための装置、プログラム、及び記録媒体

(57)【要約】
【課題】　原本データから信憑性のある抄本データを作成する抄本データ作成方法を提供する。
【解決手段】　原本ＩＤ，抜粋タグリストを含む抄本作成要求を受け取ると、原本ＩＤで指定された原本データ１１を原本記憶媒体７から読み出し、その原本データ１１について原本データ改ざん検知処理を行う。ここで、改ざんが検知されなければ、読み出した原本データから抜粋タグリストで指定されたタグに該当するデータを抜粋し、抜粋データ１２とする。さらに、原本ＩＤと抜粋タグリストを合わせて抜粋範囲データ１３とし、抜粋データ１２に抜粋範囲データ１３を合わせて抄本コンテンツデータ１４とする。抄本コンテンツデータ１４に対して抄本改ざん検知コード計算処理を行い、改ざん検知コード１５を得て、抄本コンテンツデータ１４と改ざん検知コード１５を合わせて抄本データ１６とする。最後に、抄本データ１６を抄本作成要求元に返す。



1

【特許請求の範囲】

【請求項１】　原本データから一部分を抜粋して抜粋データとし、外部から利用できない暗号鍵を使用して、該抜粋データに対する改ざん検知コードを計算し、該抜粋データと該改ざん検知コードを合わせて抄本データとすることを特徴とする抄本データ作成方法。

【請求項２】　原本データから一部分を抜粋して抜粋データとし、該抜粋した範囲を示す抜粋範囲データを作成し、外部から利用できない暗号鍵を使用して、前記抜粋データと該抜粋範囲データに対する改ざん検知コードを計算し、前記抜粋データと抜粋範囲データと該改ざん検知コードとを合わせて抄本データとすることを特徴とする抄本データ作成方法。

【請求項３】　原本データから一部分を抜粋して抜粋データとし、該抜粋した範囲を示し、且つ前記原本データの固有識別名を含めた抜粋範囲データを作成し、外部から利用できない暗号鍵を使用して、前記抜粋データと該抜粋範囲データに対する改ざん検知コードを計算し、前記抜粋データと抜粋範囲データと該改ざん検知コードとを合わせて抄本データとすることを特徴とする抄本データ作成方法。

【請求項４】　抄本を作成する原本データに対して、該原本データが改ざんされていないことを検証し、改ざんされていない場合に、前記抄本データを作成することを特徴とする請求項１乃至３のいずれか１記載の抄本データ作成方法。

【請求項５】　前記改ざん検知コードの計算に使用する前記暗号鍵は、当該抄本データ作成方法を実行させるためのプログラム内部に保持されていることを特徴とする請求項１乃至４のいずれか１記載の抄本データ作成方法。

【請求項６】　前記改ざん検知コードの計算に使用する前記暗号鍵は、当該抄本データ作成方法を実行させるためのプログラム内部に保持している暗号鍵のみによって復号可能な形で、暗号化して保持されていることを特徴とする請求項１乃至４のいずれか１記載の抄本データ作成方法。

【請求項７】　前記改ざん検知コードの計算に使用する前記暗号鍵は、当該抄本データ作成方法を実行させるためのプログラムからのみ利用可能な物理的耐タンパー性を持つ暗号処理ハードウェアの内部に保持されており、該暗号処理ハードウェアによって前記改ざん検知コードを計算することを特徴とする請求項１乃至４のいずれか１記載の抄本データ作成方法。

【請求項８】　前記原本データ、抜粋範囲データ、及び抄本データはマークアップ言語により記述されていることを特徴とする請求項１乃至７のいずれか１記載の抄本データ作成方法。

【請求項９】　請求項１乃至８のいずれか１記載の抄本データ作成方法の各工程を実行するための手段を備えた

2

抄本データ作成装置。

【請求項１０】　請求項９記載の抄本データ作成装置における抄本データを保存する手段を有する原本性保証電子保存装置。

【請求項１１】　請求項１乃至８のいずれか１記載の抄本データ作成方法における各工程を実行させるための、或いは請求項９記載又は１０記載の装置における各手段として機能させるためのプログラム。

【請求項１２】　請求項１１記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、原本データから信憑性のある抄本データを作成する抄本データ作成方法、該方法を実行させるための抄本データ作成装置、そのための装置、抄本データ作成プログラム、及び該プログラムを記録したコンピュータ読取り可能な記録媒体に関する。

【０００２】

【従来の技術】近年、あらゆる分野で情報化が高度に進展する中、法的に保存義務のある文書を紙文書としてではなく、電子文書として保存することを許可する方向へ進みつつある。そのような流れは、次の従来技術に挙げられるような原本性保証技術や、暗号処理技術を活用することにより、電子文書の信憑性を確保することが可能になりつつあるということが背景としてある。

【０００３】すなわち、小尾他：原本性保証電子保存システムの開発―基本機能の実現―, Medical Imaging Technology, Vol.１６, No.４, Proceedings of JAMIT Annual Meeting'９８（１９９８）、金井他：原本性保証電子保存システムの開発―システムの構築―, Medical Imaging Technology, Vol.１６, No.４, Proceedings of JAMIT Annual Meeting'９８（１９９８）、国分他：原本性保証電子保存システムの開発,（特）情報処理振興事業協会発行　創造的ソフトウェア育成事業及びエレクトロニック・コマース推進事業　最終成果発表会論文集　創造的ソフトウェア育成事業編（１９９８）、金井：原本性保証電子保存システムについて, Vol.３４, No.８, 行政＆ＡＤＰ（１９９８）、等の技術を活用する。

【０００４】

【発明が解決しようとする課題】そういった状況の中、電子的な原本に対して、謄本や抄本を作成したいという要求が出てくることが予想される。従来から提案されている原本性保証電子保存システムでは、原本と内容が同一であることを保証する謄本を作成することは可能であっても、原本の一部分を抜き出したものであることを保証する抄本を作成することはできなかった。しかし、例えば戸籍抄本のように、原本の一部と内容が同一であることを保証したコピーを作成したいというニーズは様々な業務において存在する。

【０００５】例えば、特開平１１－８５７９９号公報に記載の「特許抄本作成自動作成方式」では、抄本を自動的に作成することが可能になっているが、その作成された抄本が確かに原本から作成されたものであるかどうかについての保証がない。もちろん、特開平１１－８５７９９号公報に記載の発明は、特許参照の利便性を高める目的であるため、抄本の信憑性については問わないものであるが、抄本作成システムが作成する抄本に対して信憑性を求める業務も多数存在すると考えられる。

【０００６】本発明は、上述のごとき実情に鑑みてなされたものであり、電子原本（原本データ）から信憑性のある電子抄本（抄本データ）を作成する抄本データ作成方法、抄本データ作成装置、そのための装置、抄本データ作成プログラム、及び該プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することをその目的とする。

【０００７】また、本発明は、抄本を作成する際により改ざんを検知することが可能な抄本データ作成方法、抄本データ作成装置、そのための装置、抄本データ作成プログラム、及び該プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを他の目的とする。さらに、本発明は、信憑性のある電子原本から電子抄本を作成することが可能な抄本データ作成方法、抄本データ作成装置、そのための装置、抄本データ作成プログラム、及び該プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを他の目的とする。加えて、信憑性のある改ざん検知を行うことが可能な抄本データ作成方法、抄本データ作成装置、そのための装置、抄本データ作成プログラム、及び該プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを他の目的とする。

【０００８】

【課題を解決するための手段】請求項１の発明は、原本データから一部分を抜粋して抜粋データとし、外部から利用できない暗号鍵を使用して、該抜粋データに対する改ざん検知コードを計算し、該抜粋データと該改ざん検知コードを合わせて抄本データとすることを特徴としたものである。

【０００９】請求項２の発明は、原本データから一部分を抜粋して抜粋データとし、該抜粋した範囲を示す抜粋範囲データを作成し、外部から利用できない暗号鍵を使用して、前記抜粋データと該抜粋範囲データに対する改ざん検知コードを計算し、前記抜粋データと抜粋範囲データと該改ざん検知コードとを合わせて抄本データとすることを特徴としたものである。

【００１０】請求項３の発明は、原本データから一部分を抜粋して抜粋データとし、該抜粋した範囲を示し、且つ前記原本データの固有識別名を含めた抜粋範囲データを作成し、外部から利用できない暗号鍵を使用して、前記抜粋データと該抜粋範囲データに対する改ざん検知コードを計算し、前記抜粋データと抜粋範囲データと該改ざん検知コードとを合わせて抄本データとすることを特徴としたものである。

【００１１】請求項４の発明は、請求項１乃至３のいずれか１の発明において、抄本を作成する原本データに対して、該原本データが改ざんされていないことを検証し、改ざんされていない場合に、前記抄本データを作成することを特徴としたものである。

【００１２】請求項５の発明は、請求項１乃至４のいずれか１の発明において、前記改ざん検知コードの計算に使用する前記暗号鍵は、当該抄本データ作成方法を実行させるためのプログラム内部に保持されていることを特徴としたものである

【００１３】請求項６の発明は、請求項１乃至４のいずれか１の発明において、前記改ざん検知コードの計算に使用する前記暗号鍵は、当該抄本データ作成方法を実行させるためのプログラム内部に保持している暗号鍵のみによって復号可能な形で、暗号化して保持されていることを特徴としたものである。

【００１４】請求項７の発明は、請求項１乃至４のいずれか１の発明において、前記改ざん検知コードの計算に使用する前記暗号鍵は、当該抄本データ作成方法を実行させるためのプログラムからのみ利用可能な物理的耐タンパー性を持つ暗号処理ハードウェアの内部に保持されており、該暗号処理ハードウェアによって前記改ざん検知コードを計算することを特徴としたものである。

【００１５】請求項８の発明は、請求項１乃至７のいずれか１の発明において、前記原本データ、抜粋範囲データ、及び抄本データはマークアップ言語により記述されていることを特徴としたものである。

【００１６】請求項９の発明は、請求項１乃至８のいずれか１の方法の各工程を実行するための手段を備えた抄本データ作成装置である。

【００１７】請求項１０の発明は、請求項９記載の装置における抄本データを保存する手段を有する原本性保証電子保存装置である。

【００１８】請求項１１の発明は、請求項１乃至８のいずれか１の方法における各工程を実行させるための、或いは請求項９記載又は１０記載の装置における各手段として機能させるためのプログラムである。

【００１９】請求項１２の発明は、請求項１１記載のプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【００２０】

【発明の実施の形態】本発明に係る抄本データ作成処理の概要を説明する。原本を電子的に保存しておく際には、その原本データの真正性を確保するために、保存する原本データに対して暗号技術を応用した改ざん検知コードを付与するといったことが行われる。後述する本発明の一実施形態に係る電子抄本の作成方法では、まず原

本データの改ざん検知コードについてそれが正しいかどうか検証し、正しいことが分かれば、抄本作成要求元から指定された範囲のデータを原本データから抜粋する。そして抜粋したデータに対して、どの原本からどの範囲のデータを抜粋したのかを示す抄本属性データを作成し、先の抜粋データとその抄本属性データを合わせたものに対して改ざん検知コードを計算する。計算した改ざん検知コードを抜粋データ、抄本属性データとともに合わせて全体で抄本データとするものである。

【００２１】このとき、抄本データが確かに原本データから作成されたものであることを保証しているのは、抄本データに含まれている改ざん検知コードであるから、この改ざん検知コードと上記抄本データ作成プロセスとが密接に関連する必要がある。つまり、この抄本データ作成プロセスだけがこの改ざん検知コードを生成できるようにすれば、生成された抄本データが確かにこの抄本作成プロセスによって作成されたことが保証され、抄本データが原本データから作成されたことが保証されることになる。

【００２２】抄本データ作成プロセスだけが抄本の改ざん検知コードを作成できるようにするには以下に示すようないくつかの方法が考えられ、いずれの方法を採用しても良い。

（１）抄本データ作成プロセス内部に保持している暗号鍵により改ざん検知コードを計算する方法、（２）改ざん検知コードの計算に使用する暗号鍵を、抄本データ作成プロセス内部に保持している暗号鍵でのみ復号できる形で保持しておく方法、（３）改ざん検知コードの計算に使用する暗号鍵を、物理的耐タンパー性を持ったデバイスに格納し、そのデバイスへのアクセスは抄本データ作成プロセスだけしかできないように（認証が必要など）アクセスコントロールを行う方法、

【００２３】（４）抄本データ作成プロセスと改ざん検知コードの計算に使用する暗号鍵とを物理的耐タンパー性を持った同一筐体内に納める方法、（５）改ざん検知コードの計算を外部プロセスにより行うが、その外部プロセスの利用は抄本データ作成プロセスだけしかできないように（認証が必要など）アクセスコントロールを行う方法、及び、（６）改ざん検知コードの計算を外部プロセスにより行うが、抜粋データと原本データの関連についてその外部プロセスが責任をもつ（外部プロセスが抜粋データの内容を見て電子署名を付与するなど）方法。

【００２４】実際に、後から抄本データを参照すると、改ざん検知コードが付与されているため、まずその改ざん検知コードの正当性を検証する。改ざんが検知されなかった場合にはその抄本データの内容を信頼することができる。つまり、抄本データに含まれている抜粋データが、どの原本からどの範囲を抜粋したものであるのか、それが改ざん検知コードにより保証されるということになる。

【００２５】また、改ざん検知コードの種類としては、ＭＡＣ（Message Authentication Code）や、電子署名、電子公証、デジタルタイムスタンプなどがある。ＭＡＣは秘密共有鍵暗号方式、電子署名や電子公証は公開鍵暗号方式、デジタルタイムスタンプは時系列に連鎖したハッシュ方式を使用するのが一般的である。

【００２６】いずれの方式の場合にも、基本的には改ざん検知を行う対象データのハッシュ値（圧縮データ）を計算し、そのハッシュ値に対して何らかの暗号処理を施すことで改ざん検知コードとするものである。したがって、本発明の説明では特に断らない限り改ざん検知コードはＭＡＣ、電子署名、電子公証、デジタルタイムスタンプのいずれの技術でも適用できるものとする。ただし、各方式では、改ざん検知コードの検証の仕方が異なるが、検証方式は本発明の特徴ではないため、その違いについては区別して説明しない。

【００２７】また、本発明では抄本を作成する原本データの内容について、そのデータフォーマットは規定していないが、データフォーマットが規定されている場合、例えば原本データ等がマークアップ言語であるＸＭＬにより記述されている場合には、抄本データ作成プロセスがそのデータフォーマットをパース可能となり、より便利な抄本データ作成機能が提供できることとなる。

【００２８】次に、本発明の実施形態に係る抄本作成方法をそれを実行するための装置と共に詳細に説明する。図１は、本発明に係る抄本データ作成処理を実行するための抄本データ作成装置の概要を示す図で、図中、１０は抄本データ作成装置、２０は抄本データ作成装置１０にネットワークで接続された外部システムである。抄本データ作成装置１０は、暗号処理ボード２、抄本記憶媒体３、プロセッサ４、内部記憶媒体５、プログラム格納媒体６、原本記憶媒体７を具備している。

【００２９】プログラム格納媒体６は、主制御プログラム、本発明に係る抄本データ作成プログラムなどの各種プログラムを格納可能なメモリであり、たとえば書換可能なＥＥＰＲＯＭや読み出し専用のＲＯＭなどからなる。プロセッサ４は、プログラム格納媒体６に格納された各種プログラムを読み出して実行する制御装置である。内部記憶媒体５は、各種プログラムの実行に必要となるパラメータを記憶するＥＥＰＲＯＭなどからなるメモリである。抄本記憶媒体３及び原本記憶媒体７は光ディスク等耐久年数が長い記憶媒体であることが好ましく、原本記憶媒体７は外部に設置され、当該抄本データ作成装置１０から認証により原本を読み出せるような構成としてもよい。抄本記憶媒体３は、例えば外部システム２０からの抄本データ作成要求に応じて作成した抄本データを、通信ポートを介して送信する前に一時的に格納する記憶媒体としてもよいし、原本データから前もって抄本データを作成したものを保管する記憶媒体として

もよい。なお、各記憶媒体５，６，７は、本発明を適用する環境に応じて一体としてもよいことはいうまでもない。

【００３０】また、図１で示す実施形態においては、暗号処理を行う暗号処理ボード２を組み込み、暗号処理ボード２で鍵生成，鍵保管，暗号化，復号化の処理を行っているが、プログラム格納媒体６に鍵生成プログラム，暗号化プログラム，復号化プログラムなどを格納し、プロセッサ４によってそれらプログラムを実行する方式としてもよい。その際、鍵生成プログラムにより生成された、或いは外部で生成した暗号鍵を暗号処理ボード２のようなハードウェアを使用してハードウェア内部に安全に保管するか、抄本データ作成及び検証するプログラム内部に保管することが好ましい。なお、本発明においては鍵の生成に関するモジュール，プログラムは具備しなくてもよい。

【００３１】図２は、本発明の一実施形態に係る抄本データ作成処理の概要を説明するための図で、図中、１１は原本データ、１２は抜粋データ、１３は抜粋範囲データ、１４は抄本コンテンツデータ、１５は改ざん検知コード、１６は抄本データ、７は原本データを格納してある原本記憶媒体である。以下、原本から抄本を作成する方法について、図面を参照して非常に単純な例で説明しているが、現実的には、特開平１１－８５７９９号公報「特許抄本作成自動作成方式」にあるような複雑な抄本作成方法を採用することになる。

【００３２】図３は、本発明の一実施形態に係る抄本データ作成方法を説明するためのフロー図である。抄本データを作成するには、まず、抄本を作成する原本データ１１を原本記憶媒体７から読み出す。次に、原本データ１１から一部分を抜粋して抜粋データ１２とし（ステップＳ１）、外部から利用できない暗号鍵を使用して、抜粋データ１２に対する改ざん検知コード１５を計算し（ステップＳ２）、抜粋データ１２と改ざん検知コード１５を合わせて抄本データ１６とする（ステップＳ３）。なお、原本データ１１，抄本データ１６がマークアップ言語により記述されていることが好ましい。

【００３３】図４は、本発明の他の実施形態に係る抄本データ作成方法を説明するためのフロー図である。本実施形態においては、まず、原本記憶媒体７から読み出した原本データ１１から一部分を抜粋して抜粋データ１２とし（ステップＳ１１）、抜粋した範囲を示す抜粋範囲データ１３を作成する（ステップＳ１２）。次に、外部から利用できない暗号鍵を使用して、抜粋データ１２と抜粋範囲データ１３、即ち抄本コンテンツデータ１４に対する改ざん検知コード１５を計算し（ステップＳ１３）、抜粋データ１２と抜粋範囲データ１３と改ざん検知コード１５とを合わせて抄本データ１６とする（ステップＳ１４）。さらに、本実施形態において、抜粋範囲データ１３を作成する際に原本データ１１の固有識別名を含めたものとしてもよい。なお、原本データ１１，抜粋範囲データ１３，抄本データ１６がマークアップ言語により記述されていることが好ましい。

【００３４】図５は、本発明の他の実施形態に係る抄本データ作成方法を説明するためのフロー図である。本実施形態においては、まず、原本記憶媒体７から読み出した原本データ１１が改ざんされていないことを検証し（ステップＳ２１）、改ざんが無いかを判断し（ステップＳ２２）、改ざんが有れば処理を終了し、無ければ上述の各実施形態に従って抄本データ１６を作成する（ステップＳ２３）。

【００３５】本発明の他の実施形態に係る抄本データ作成方法においては、前述のごとく改ざん検知コード１５の計算に使用する暗号鍵が抄本データ作成方法を実行するプログラム内部に保持されており、該暗号鍵が外部から利用できないようにしている。さらに、改ざん検知コード１５の計算に使用する暗号鍵が、抄本データ作成方法を実行するプログラム内部に保持している暗号鍵のみによって復号可能な形で、暗号化して保持されているようにしてもよい。さらに、改ざん検知コード１５の計算に使用する暗号鍵が、抄本データ作成方法を実行するプログラムからのみ利用可能な物理的耐タンパー性を持つ暗号処理ハードウェアの内部に保持されており、該ハードウェアによって改ざん検知コード５を計算するようにしてもよい。

【００３６】前述のごとく、本発明は基本的には改ざん検知を行う対象データのハッシュ値（圧縮データ）を計算し、そのハッシュ値に対して何らかの暗号処理を施すことで改ざん検知コードとするものであり、特に断らない限り改ざん検知コードはＭＡＣ，電子署名，電子公証，デジタルタイムスタンプのいずれの技術でも適用できるものとする。しかし、以下の例では抄本データ作成プロセス自身が持つ署名鍵を使用した電子署名を改ざん検知コードとする方法について説明する。また、各方式では、改ざん検知コードの検証の仕方が異なるが、検証方式は本発明の特徴ではないため、その違いについては区別して説明しない。また、前述のごとく、本発明では抄本を作成する原本データの内容について、そのデータフォーマットは規定していないが、以下の説明では、原本データがマークアップ言語であるＸＭＬにより記述されているものとして説明する。

【００３７】図６は、本発明の一実施形態に係る抄本データ作成処理の一例を説明するための図である。前述の抄本作成プロセスにより実行される抄本作成処理として、原本ＩＤ，抜粋タグリストを含む抄本作成要求を受け取ると、まず、原本ＩＤで指定された原本データ１１を原本記憶媒体７から読み出し、読み出した原本データ１１について「原本データ改ざん検知処理」を行う。ここで、改ざんされていると判断された場合にはエラーを返して処理を終了する。改ざんが検知されなければ、読

み出した原本データから抜粋タグリストで指定されたタグに該当するデータを抜粋し、抜粋データ１２とする。さらに、原本ＩＤと抜粋タグリストを合わせて抜粋範囲データ１３とし、抜粋データ１２に抜粋範囲データ１３を合わせて抄本コンテンツデータ１４とする。抄本コンテンツデータ１４に対して、以下に示す「抄本改ざん検知コード計算処理」を行い、改ざん検知コード１５を得て、抄本コンテンツデータ１４と改ざん検知コード１５を合わせて抄本データ１６とする。最後に、抄本データ１６を抄本作成要求元に返し、処理を終了する。

【００３８】図７は、図６の原本データ改ざん検知処理の一例を説明するための図である。まず、原本データ１１を原本コンテンツデータと改ざん検知コードに分離する。次に、原本コンテンツデータに対してハッシュ値を計算する。改ざん検知コードを、システムが保持する公開鍵で復号して検証ハッシュ値とし、先のハッシュ値と検証ハッシュ値が異なる場合にはエラーで終了し、一致した場合には正常に終了したものとする。

【００３９】図８は、図６の抄本データ作成処理における抄本改ざん検知コード計算処理（１）を説明するための図である。まず、抄本コンテンツデータ１４に対してハッシュ値を計算し、プロセスが保持する署名鍵によりハッシュ値を暗号化して電子署名とする。次に、電子署名を改ざん検知コード１５として返す。

【００４０】図９は、図６の抄本データ作成処理における抄本改ざん検知コード計算処理（２）を説明するための図である。まず、抄本コンテンツデータ１４に対してハッシュ値を計算し、システムが保持する暗号化秘密鍵を取得する。次に、プロセスが保持する秘密鍵により暗号化秘密鍵を復号して署名鍵とし、署名鍵によりハッシュ値を暗号化して電子署名とする。さらにその電子署名を改ざん検知コード１５として返す。

【００４１】図１０は、図６の抄本データ作成処理における抄本改ざん検知コード計算処理（３）を説明するための図である。まず、抄本コンテンツデータ１４に対してハッシュ値を計算し、暗号処理ボードに対してプロセスの認証を行う。認証が失敗したときにはエラーを返して終了し、認証できたときには暗号処理ボードにハッシュ値を渡し、暗号処理ボードに格納されている署名鍵でハッシュ値を暗号化して電子署名とする。さらにその電子署名を改ざん検知コード１５として返す。なお、暗号処理ボードは、ＩＣカードでも良い。そのＩＣカードの所有者が例えば、抄本の作成に責任を持つ担当者であっても良い。その場合、抄本作成要求の中に、ＩＣカードへのパスワードも含めて受け取る。

【００４２】図１１は、図６の抄本データ作成処理における抄本改ざん検知コード計算処理（４）を説明するための図である。まず、抄本コンテンツデータ１４に対してハッシュ値を計算し、電子公証サービスに対してプロセスの認証を行う。認証が失敗したときにはエラーを返して終了し、成功したときには電子公証サービスにハッシュ値を渡し、電子公証サービスから電子公証データを受け取る。さらに電子公証データを改ざん検知コード１５として返す。

【００４３】図１２は原本データの一例を示す図、図１３は抄本作成要求に含まれるパラメータの一例を示す図、図１４は抜粋データの一例を示す図、図１５は抜粋範囲データの一例を示す図、図１６は抄本データの一例を示す図である。原本データにはそのコンテンツに加え、例えばＩＤ，タイトル，作成者，要約等がその言語の形式で記述されている（図１２参照）。なお、ここでは、原本データの改ざん検知コード<signature>として電子署名がdocument.p7というファイルに記録されていることを示している。

【００４４】抄本作成要求には、例えば、原本データの原本ＩＤ、抜粋タグリストとしてtitle, name, addressをパラメータとして含んでいる（図１３参照）。抄本作成要求に対する抜粋データとしては、抜粋タグリストとそれらに関わる抜粋情報title, name, addressとが含まれている（図１４参照）。抜粋範囲データとしては、例えばデータのＩＤと上記title, name, addressの記載の場所に係わるタグが記録されている（図１５参照）。抄本データには、抜粋データ及び抜粋範囲データに加え、抄本データの改ざん検知コード<signature>が記述されている（図１６参照）。なお、ここでは、抄本データの改ざん検知コード<signature>として電子署名がabstract.p7というファイルに記録されることを示している。

【００４５】以上、本発明の抄本データ作成方法に係る各実施形態を中心に説明してきたが、本発明は、上記方法の各工程を実行するための手段を構成要素とする抄本データ作成装置としても実現可能である。また、本発明は、この各処理に係る各手段を実行可能に備えた抄本データ作成装置と同様に、該抄本データ作成装置と該装置において作成した抄本データを保存する手段とを有する原本性保証電子保存装置、コンピュータに抄本データ作成方法を実行させるためのプログラム、及び該プログラムを記録したコンピュータ読取り可能な記録媒体としての形態も可能である。

【００４６】本発明による抄本データ作成の各処理を実現するためのプログラムやデータを記憶した記録媒体の実施形態を説明する。記録媒体としては、具体的には、ＣＤ－ＲＯＭ、光磁気ディスク、ＤＶＤ－ＲＯＭ、フロッピー（登録商標）ディスク、フラッシュメモリ、及びその他各種ＲＯＭやＲＡＭ等が想定でき、これら記録媒体に上述した本発明の各実施形態に係る各処理をコンピュータに実行させ、抄本データ作成の機能を実現するためのプログラムを記録して流通させることにより、当該機能の実現を容易にする。そしてコンピュータ等の情報処理装置に上記のごとくの記録媒体を装着して情報処理

11

装置によりプログラムを読み出すか、若しくは情報処理装置が備えている記憶媒体に当該プログラムを記憶させておき、必要に応じて読み出すことにより、本発明に係わる抄本データ作成機能を実行することができる。

【００４７】

【発明の効果】本発明によれば、本発明による抄本データ作成プロセスのみが抄本の改ざん検知コードを作成できるようにしているので、電子原本（原本データ）から信憑性のある電子抄本（抄本データ）を作成することが可能となる。さらに、信憑性のある電子原本から前記電子抄本を作成することが可能となる。

【図面の簡単な説明】

【図１】　本発明に係る抄本データ作成処理を実行するための抄本データ作成装置の概要を示す図である。

【図２】　本発明の一実施形態に係る抄本データ作成処理の概要を説明するための図である。

【図３】　本発明の一実施形態に係る抄本データ作成方法を説明するためのフロー図である。

【図４】　本発明の他の実施形態に係る抄本データ作成方法を説明するためのフロー図である。

【図５】　本発明の他の実施形態に係る抄本データ作成方法を説明するためのフロー図である。

【図６】　本発明の一実施形態に係る抄本データ作成処理の一例を説明するための図である。

【図７】　図６の原本データ改ざん検知処理の一例を説明するための図である。

12

【図８】　図６の抄本データ作成処理における抄本改ざん検知コード計算処理（１）を説明するための図である。

【図９】　図６の抄本データ作成処理における抄本改ざん検知コード計算処理（２）を説明するための図である。

【図１０】　図６の抄本データ作成処理における抄本改ざん検知コード計算処理（３）を説明するための図である。

【図１１】　図６の抄本データ作成処理における抄本改ざん検知コード計算処理（４）を説明するための図である。

【図１２】　原本データの一例を示す図である。

【図１３】　抄本作成要求に含まれるパラメータの一例を示す図である。

【図１４】　抜粋データの一例を示す図である。

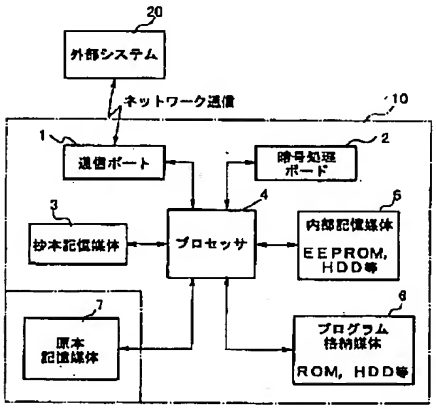
【図１５】　抜粋範囲データの一例を示す図である。

【図１６】　抄本データの一例を示す図である。

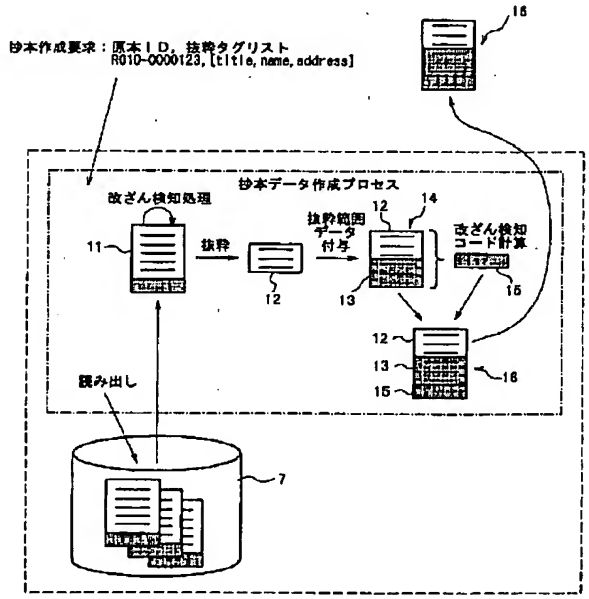
【符号の説明】

１…通信ポート、２…暗号処理ボード、３…抄本記憶媒体、４…プロセッサ、５…内部記憶媒体、６…プログラム格納媒体、７…大容量記憶媒体（原本記憶媒体）、１０…抄本データ作成装置、１１…原本データ、１２…抜粋データ、１３…抜粋範囲データ、１４…抄本コンテンツデータ、１５…改ざん検知コード、１６…抄本データ、２０…外部システム。

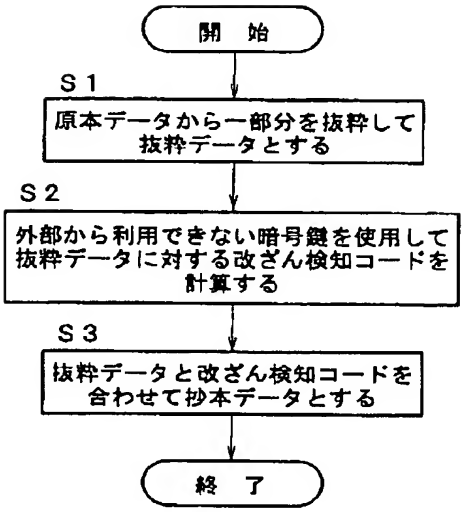
【図１】



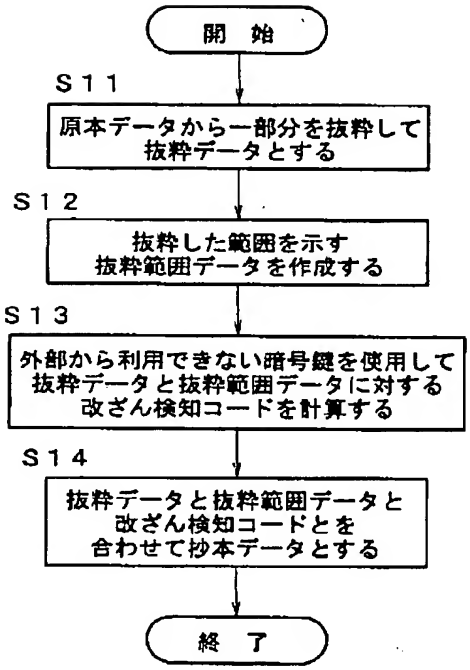
【図２】



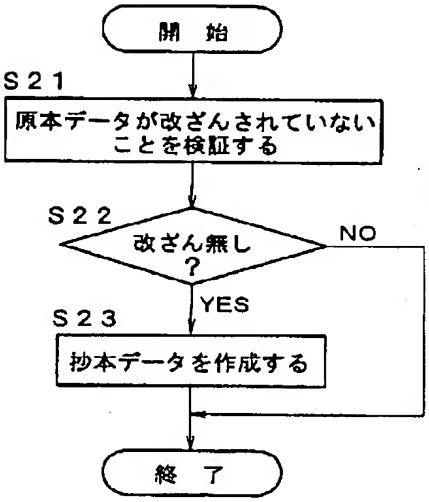
【図３】



【図４】



【図５】



【図６】

抄本データ作成処理（抄本データ作成プロセスにより実行される）

```
原本ID、抜粋タグリストを含む抄本作成要求を受け取る
原本IDで指定された原本データを原本記憶媒体から読み出す
読み出した原本データについて「原本データ改ざん検知処理」を行う
if(改ざんされている){
        エラーを返して終了
}
読み出した原本データから抜粋タグリストで指定されたタグに該当するデータを抜粋し、抜粋データとする
原本IDと抜粋タグリストを合わせて抜粋範囲データとする
抜粋データに抜粋範囲データを合わせて抄本コンテンツデータとする
抄本コンテンツデータに対して「抄本改ざん検知コード計算処理」を行い、改ざん検知コードを得る
抄本コンテンツデータと改ざん検知コードを合わせて抄本データとする
抄本データを抄本作成要求元に返す
正常に終了
```

【図７】

原本データ改ざん検知処理

```
原本データを原本コンテンツデータと改ざん検知コードに分離する
原本コンテンツデータに対してハッシュ値を計算する
改ざん検知コードを、システムが保持する公開鍵で復号して検証ハッシュ値とする
if(先のハッシュ値と検証ハッシュ値が異なる){
        エラーで終了
}
else{
        正常に終了
}
```

【図８】

抄本改ざん検知コード計算処理（１）

```
抄本コンテンツデータに対してハッシュ値を計算する
プロセスが保持する署名鍵によりハッシュ値を暗号化して電子署名とする
電子署名を改ざん検知コードとして返す
```

【図９】

抄本改ざん検知コード計算処理（２）

```
抄本コンテンツデータに対してハッシュ値を計算する
システムが保持する暗号化秘密鍵を取得する
プロセスが保持する秘密鍵により暗号化秘密鍵を復号して署名鍵とする
署名鍵によりハッシュ値を暗号化して電子署名とする
電子署名を改ざん検知コードとして返す
```

【図１０】

抄本改ざん検知コード計算処理（３）

```
抄本コンテンツデータに対してハッシュ値を計算する
暗号処理ボードに対してプロセスの認証を行う
if(認証が失敗した){
        エラーを返して終了
}
暗号処理ボードにハッシュ値を渡す
暗号処理ボードに格納されている署名鍵でハッシュ値を暗号化して電子署名とする
電子署名を改ざん検知コードとして返す
```

【図１１】

抄本改ざん検知コード計算処理（４）

```
抄本コンテンツデータに対してハッシュ値を計算する
電子公証サービスに対してプロセスの認証を行う
if(認証が失敗した){
        エラーを返して終了
}
電子公証サービスにハッシュ値を渡す
電子公証サービスから電子公証データを受け取る
電子公証データを改ざん検知コードとして返す
```

【図１２】

原本データの例

```
<?xml version="1.0" encoding="Shift-JIS"?>
<document>
        <identifier>R010-0000123</identifier>
        <title>特許について</title>
        <name>理光 太郎</name>
        <address>横浜市</address>
        <abstract>特許について記述したものである。</abstract>
        <contents>
発明届出書について
はじめに発明届出書の作成手順について説明する。発明届出書は、、、
        </contents>
        <signature>document.p7</signature>
</document>
```

【図１３】

抄本作成要求に含まれるパラメータの例

```
原本ID: R010-0000123
抜粋タグリスト: title, name, address
```

【図１４】

抜粋データの例

```
<title>特許について</title>
<name>理光 太郎</name>
<address>横浜市</address>
```

【図１５】

抜粋範囲データの例

```
<extract>
        <docid>R010-0000123</docid>
        <tags>
                <li>title</li>
                <li>name</li>
                <li>address</li>
        </tags>
</extract>
```

【図１６】

抄本データの例

```
<?xml version="1.0" encoding="Shift-JIS"?>
<document>
<extract>
        <docid>R010-0000123</docid>
        <tags>
                <li>title</li>
                <li>name</li>
                <li>address</li>
        </tags>
</extract>
        <title>特許について</title>
        <name>理光 太郎</name>
        <address>横浜市</address>
        <signature>abstract.p7</signature>
</document>
```

フロントページの続き

(51)Int.Cl.[7]	識別記号	F I		ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０９Ｃ 1/00	６４０	Ｇ０９Ｃ 1/00	６４０Ａ	
// Ｇ０６Ｆ 17/30	１２０	Ｇ０６Ｆ 17/30	１２０Ａ	

Ｆターム(参考) 5B017 AA02 BA07 CA16
5B075 KK54 KK66 NS10
5B082 GA11
5J104 AA08 LA02 NA02